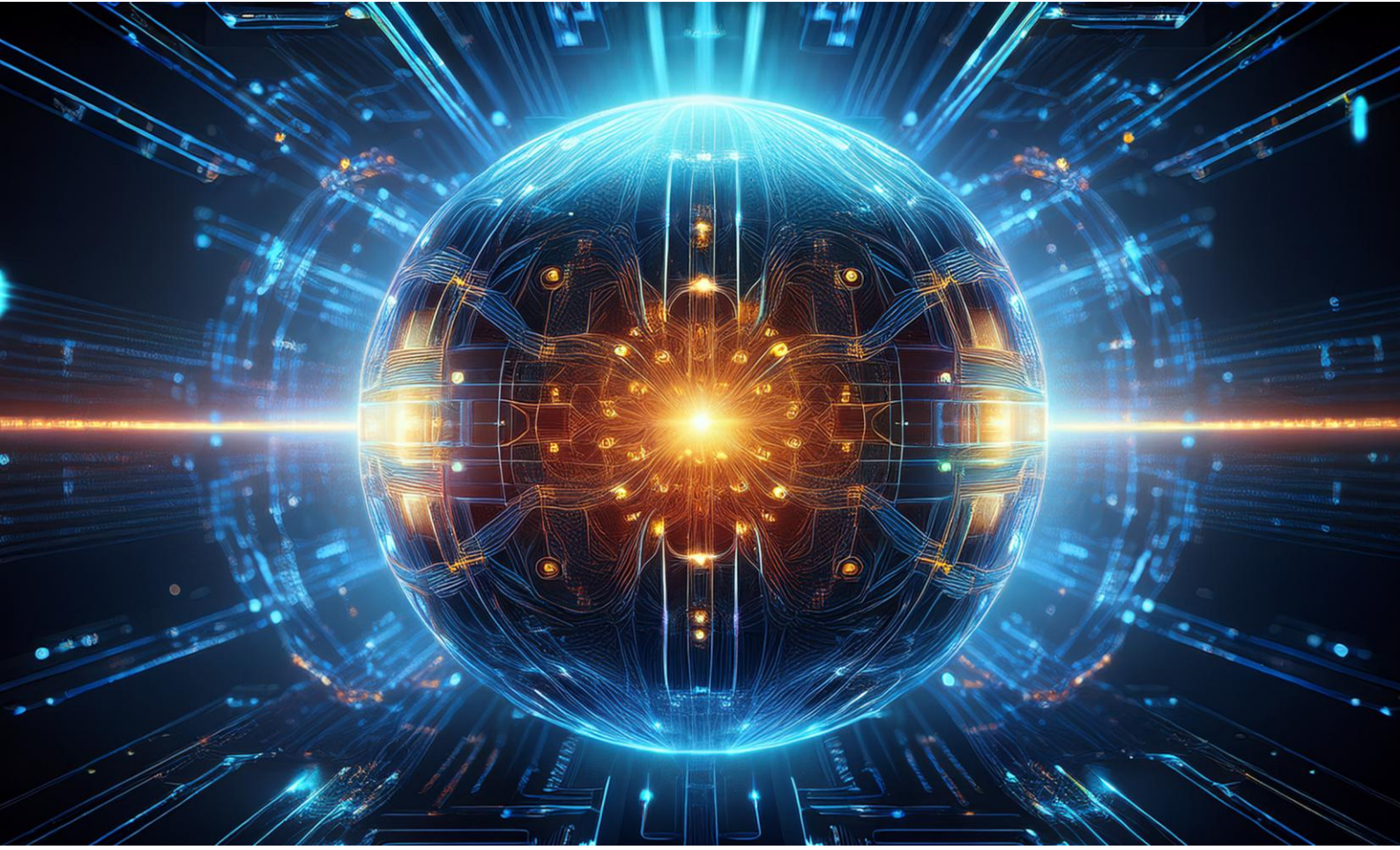


Post-Quantum-Migration: Lösungen für eine quanten-sichere Infrastruktur

SAMA PARTNERS Business Solutions GmbH
29.08.2025

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

Inhalt

Einleitung 2
Warum sind aktuelle, asymmetrische kryptografische Verfahren nicht post-quantensicher? ..3
Das Mosca-Theorem 4
Moscas x-y-z Quantenrisikomodell: Eine Methodik für die Bewertung von Quantenrisiken 5
Store Now, Decrypt Later 5
Lange Migrationszeiträume bei komplexen Systemen 6
Daten zukunftssicher verschlüsseln – über Post-Quantum Migration 6
Kryptographie-Inventar....6
Quantum Key Distribution 7
Ziele einer Migration auf Basis einer QKD-Implementierung in Unternehmen 7
Welche Maßnahmen sind bei einer Post-Quantum Migration umzusetzen? 7
Die 4 Phasen einer Post-Quantum Migration 8
Zusammenfassung 9
Verweise....11

Einleitung

Bis vor kurzem wurde die Quanteninformatik oft als eine Fähigkeit angesehen, die in der Zukunft auftauchen könnte, als fast etwas, das in einen Science-Fiction-Roman gehört.

Die Wissenschaft, die Quantencomputern zugrunde liegt, hat ihren Ursprung in der Physik der Quantenmechanik, die unser Verständnis des Universums grundlegend verändert hat. Die Konzepte lassen sich mitunter nur schwer mit der Welt, in der wir leben, in Einklang bringen. Selbst viele Physiker hatten Schwierigkeiten mit diesen revolutionären Ideen, aber Experimente und Beobachtungen haben die Quantentheorie bestätigt, und die ihr zugrunde liegenden Prinzipien sind in alltäglichen Geräten wie Lasern und Transistoren offensichtlich. Auf die Quanteninformatik bezogen kann in einem Quantencomputer ein QBit gleichzeitig Null und Eins sein, entgegen der derzeitigen klassischen binären (1 oder Null) Bits. Diese bisherigen auf quantenmechanische Prinzipen basierende Technologien lassen das Potenzial der Quantenphysik nur erahnen. Bis zum Meilenstein eines ersten, vollfunktionsfähigen Quantencomputers ist jedoch noch viel Arbeit nötig.

Dieser Meilenstein liegt wahrscheinlich noch ein Jahrzehnt oder mehr in der Zukunft, aber die Arbeit wird von vielen Forschern auf der ganzen Welt intensiv verfolgt, da die Quantentechnologie neben dem Einsatz in der Computertechnologie auch Vorteile in einer Vielzahl von anderen Bereichen wie z.B. in Sensoren, in der Kommunikation und der Optik verspricht.

Bereits 1994 beschrieb der Mathematiker Peter Shor einen Algorithmus, der es zukünftigen Quantencomputern ermöglicht, extrem schwierige mathematische Probleme, wie z. B. die Faktorisierung sehr großer Zahlen, zu lösen. 1996 entwickelte der indisch-amerikanische Physiker und Informatiker Lov Grover einen weiteren Quantenalgorithmus, um die Suche in unstrukturierten Datenbanken oder Listen effizienter durchzuführen. Probleme, wie die Suche in unstrukturierten Datenbanken, das „Rucksackproblem“ oder „Travelling Salesman Problem“, sind mit den heutigen Computern im Grunde unlösbar. Die zugrunde liegenden Rechenoperationen sind auf aktuellen, realen Rechnern so ineffizient, dass die Lösung dieser Probleme sehr viel Zeit in Anspruch nimmt und sie durch diese Eigenschaft zur mathematischen Grundlage der am häufigsten verwendeten Verschlüsselungssysteme in der Computertechnologie geworden sind. Beide Algorithmen revolutionierten das Verständnis darüber, wie Quantencomputer bestimmte Probleme, wie z.B. dem Brechen von Kryptoverfahren, effizienter lösen können.

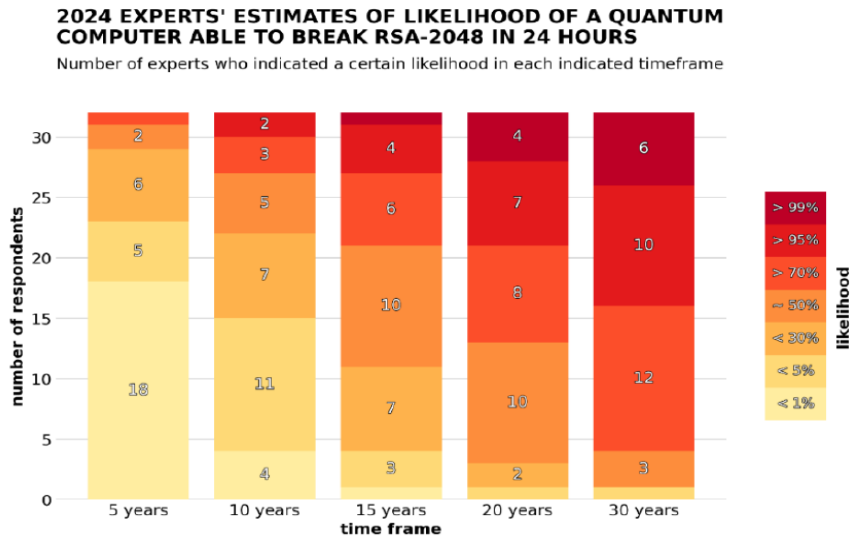
Sobald aber kryptographisch relevanten Quantencomputer (CRQC) verfügbar sind, werden sie die bis dato als sicher geltenden Verschlüsselungssysteme mit öffentlichem Schlüssel im Wesentlichen effizient brechen können. Auch traditionellere Verschlüsselungssysteme mit gemeinsamem Schlüssel (wie AES) werden davon betroffen sein und ihre effektive Sicherheitsstärke, was wir heute als sicher ansehen, auf etwa die Hälfte dessen reduzieren. Dies wird verheerende Auswirkungen auf Systeme haben, die zum Schutz der elektronischen Kommunikation und digitaler Transaktionen eingesetzt werden. Die meisten sicheren Internet-Prozesse beruhen auf Protokollen, die Kryptographie mit öffentlichen Schlüsseln verwenden, einschließlich derjenigen, die zur Sicherung von Websites, für Banktransaktionen, sichere E-Mails und digitale Signaturen verwendet werden, deren Sicherheitsstärke zukünftig besonders gefährdet ist.

Warum sind aktuelle, asymmetrische kryptografische Verfahren nicht post-quantensicher?

Zwei weit verbreitete, asymmetrische Kryptoverfahren, die zur Sicherung von Daten und Kommunikation verwendet werden sind RSA (Rivest-Shamir-Adleman) und ECC (Elliptic Curve Cryptography). Beide Algorithmen sind jedoch anfällig für Angriffe durch Quantencomputer.

RSA (Rivest-Shamir-Adleman)

- **Art**: Asymmetrische Kryptografie
- **Funktionsweise**: RSA basiert auf der mathematischen Schwierigkeit der Faktorisierung großer Primzahlen. Es verwendet ein Schlüsselpaar: einen öffentlichen Schlüssel, der zum Verschlüsseln von Nachrichten verwendet wird, und einen privaten Schlüssel, der zum Entschlüsseln dieser Nachrichten dient.
- **Sicherheit**: Die Sicherheit von RSA beruht auf der Annahme, dass es schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen. Mit zunehmender Schlüssellänge (z.B. 2048 oder 4096 Bit) wird die Sicherheit erhöht.
- **Verwendung**: RSA wird häufig für den sicheren Austausch von Schlüsseln, digitale Signaturen und in SSL/TLS-Zertifikaten verwendet.
- **Herausforderung**: Quantencomputer können durch Verwendung von Shor‘s Algorithmus die Faktorisierung großer Zahlen exponentiell beschleunigen. Während klassische Computer bei sehr großen Zahlen (z.B. 2048 Bit) Jahrzehnte oder Jahrhunderte benötigen, um sie zu faktorisieren, kann ein ausreichend leistungsfähiger Quantencomputer dies in polynomialer Zeit erledigen.
- **Folge**: Wenn ein Quantencomputer in der Lage ist, den Shor-Algorithmus auszuführen, könnte er den privaten Schlüssel aus dem öffentlichen Schlüssel ableiten, was die gesamte Sicherheit von RSA aufhebt.



In einer Umfrage des Global Risk Institute und dem Kanadisch-Deutschen Unternehmen evolutionQ, aus dem Jahr 2024 unter 32 internationalen Kryptografie-Experten prognostizierten die 16 Teilnehmer der Studie, dass die Wahrscheinlichkeit, dass Quantenrechner in spätestens 30 Jahren in der Lage sein werden, eine RSA-2048-Bit-Verschlüsselung in weniger als 48 Stunden entschlüsseln zu können, bei über 95% liegt.

ECC (Elliptic Curve Cryptography)

- **Art**: Asymmetrische Kryptografie
- **Funktionsweise**: ECC basiert auf den mathematischen Eigenschaften elliptischer Kurven über endlichen Körpern. Wie bei RSA gibt es auch hier ein Schlüsselpaar (öffentlicher und privater Schlüssel), aber ECC kann mit deutlich kürzeren Schlüssellängen eine vergleichbare Sicherheit bieten.
- **Sicherheit**: Die Sicherheit von ECC beruht auf der Schwierigkeit des Diskreten Logarithmusproblems elliptischer Kurven. Zum Beispiel bietet ein 256-Bit-ECC-Schlüssel eine ähnliche Sicherheit wie ein 3072-Bit-RSA-Schlüssel.
- **Verwendung**: ECC wird zunehmend in modernen Anwendungen eingesetzt, insbesondere in mobilen Geräten und IoT (Internet of Things), da es weniger Rechenleistung benötigt und effizienter ist.
- **Herausforderung**: Ähnlich wie bei RSA kann ein Quantencomputer mit Shors Algorithmus auch das Diskrete Logarithmusproblem effizient lösen. Das gilt sowohl für das klassische Diskrete Logarithmusproblem in Gruppen als auch speziell für elliptische Kurven.
- **Folge**: Wenn ein ausreichend leistungsfähiger Quantencomputer existiert, könnte er den Shor-Algorithmus verwenden, um den privaten Schlüssel aus dem öffentlichen Schlüssel zu berechnen. Damit wäre die Sicherheit von ECC gebrochen, und die Verschlüsselung oder Signaturen könnten kompromittiert werden. Dies hebt die Sicherheit von ECC in einer Welt mit leistungsfähigen Quantencomputern auf und macht es notwendig, auf quantensichere Kryptografie umzusteigen.

Das Mosca-Theorem

Das Mosca-Theorem ist ein bedeutendes Ergebnis im Bereich der Quantenkryptographie und des Quantenrisikos, das von dem Kanadischen Physiker und Kryptographen Dr. Michele Mosca in den frühen 2000er Jahren formuliert wurde. Es beschreibt die Beziehung zwischen der Entwicklung leistungsfähiger Quantencomputer und der Sicherheit klassischer kryptografischer Systeme.

Das Mosca-Theorem besagt, dass sobald leistungsfähige, kryptographisch relevante Quantencomputer (CRQC) existieren, viele heute verwendete asymmetrische Verschlüsselungsverfahren (wie RSA, ECC) sofort kompromittiert werden können. Denn Quantenalgorithmen, wie z.B. Shors Algorithmus, ermöglichen es, die neu entstandene Sicherheitslücke bei asymmetrischer Kryptographie, nämlich die der einfachen Faktorisierung großer Zahlen, sehr effizient durchzuführen. Ähnliches gilt bei der symmetrischen Verschlüsselung, die durch die effizientere Lösung diskreter Logarithmen mit Hilfe von Grovers Quantenalgorithmus beschleunigt wird. Damit könnten Angreifer verschlüsselte Nachrichten, die aktuell noch mit RSA oder ECC bzw. mit AES gesichert sind, in kurzer Zeit entschlüsseln.

Um dieses Risiko zu mindern, wird als Schutzmaßnahme empfohlen, auf quantenresistente Verschlüsselungsverfahren – auf die sogenannten Post-Quanten-Kryptographie (PQC) – umzusteigen, da die Bedrohung durch Quantencomputer unmittelbar nach ihrer Verfügbarkeit besteht. Quantenresistente Verschlüsselungsverfahren basieren auf Problemen, die auch mit Quantencomputern nur schwer lösbar sind.

Das Theorem hebt ebenso hervor, dass die Gefahr durch Quantencomputer nicht nur theoretisch ist, sondern praktisch unmittelbar wird, sobald diese leistungsfähig genug sind. Es betont die Notwendigkeit einer proaktiven Anpassung der Sicherheitsinfrastrukturen im Zeitalter der Quanten.

Moscas x-y-z Quantenrisikomodell: Eine Methodik für die Bewertung von Quantenrisiken

Das x-y-z-Modell zur Bewertung des Quantenrisikos ist ein konzeptioneller Rahmen des Mosca-Theorems, der dazu dient, die Risiken im Zusammenhang mit Quantencomputern und ihrer potenziellen Bedrohung für bestehende kryptografische Systeme zu analysieren. Hierbei werden drei Zeiträumen betrachtet, die dazu dienen, das Risiko für eine Gefahr durch die kriminelle Nutzung von Quantencomputern einzuschätzen und den Zeitpunkt zu bestimmen, bei dem ein Handlungsbedarf besteht, Daten post-quantensicher zu machen.

Die drei Zeiträume sind wie folgt definiert:

- Die **Haltbarkeitszeit x**: Wie viele Jahre müssen sensible Daten sicher bleiben?
- Die **Migrationszeit y**: Wie viele Jahre wird es dauern, die Systeme und Protokolle, die diese Daten schützen, sicher aufzurüsten?
- Die **Bedrohungszeit z**: Die geschätzte Zeit, bis potenzielle Angreifer Zugang zu Quantencomputern von kryptografischer Bedeutung erhalten

Abb.1 : Moscas x-y-z Quantenrisikomodell

Wenn sich die Summe aus x + y dem Zeitraum z nähert, gilt es, sofort zu handeln und die Verschlüsselung sensibler Daten über eine entsprechende Migration post-quantum sicher zu machen.

Store Now, Decrypt Later

Die Fortschritte in der Quanteninformatik, insbesondere bei der Fehlerkorrektur, haben die Einschätzung der Verfügbarkeit von kryptografisch relevanten Quantencomputern verkürzt, so dass die verbleibende Zeit für die Umstellung auf quantensichere Kryptografie kurz ist. Insbesondere Daten, die langfristig geschützt werden müssen, sind bereits jetzt durch die sogenannte „SNDL-Bedrohung“ (Store Now, Decrypt Later) gefährdet. Die SNDL-Bedrohung beschreibt eine Sicherheitsgefahr, bei der Angreifer schon heute verschlüsselte Daten sammeln, um diese mit Hilfe von

Quantencomputern zu einem späteren Zeitpunkt zu entschlüsseln. Besonders bei sensiblen Daten wie Geschäftsgeheimnissen, Gesundheitsinformationen oder staatlichen Geheiminformationen besteht die Gefahr, dass diese in der Zukunft rückwirkend kompromittiert werden.

Lange Migrationszeiträume bei komplexen Systemen

Ein weiteres Bedrohungsszenario entsteht aus den langen Migrationszeiträumen, die bei komplexen Systemen wie z.B. bei Public-Key-Infrastrukturen (PKI) oder Geräten mit langer Lebensdauer auftreten. Selbst wenn ein System nicht von laufenden Angriffen betroffen ist, wie im SNDL-Szenario, so besteht dennoch die Gefahr, dass der Übergang zur quantensicheren Kryptografie nicht rechtzeitig abgeschlossen wird und die Vertraulichkeit und Authentizität der gesamten Kommunikation gefährdet ist.

Daten zukunftssicher verschlüsseln – über Post-Quantum Migration

Die Post-Quantum Migration bezieht sich auf den Prozess der Anpassung und Migration von aktuellen Informationssystemen, Daten und Kommunikationsprotokollen, um sie gegen die zukünftigen Bedrohungen durch Quantencomputer abzusichern. Sie setzt dabei auf Verschlüsselungsmethoden, wie z.B. der Post-Quantum Cryptography (PQC) oder der Quantum Key Distribution (QKD), die auch der Rechenleistung von Quantencomputern standhalten. Hierbei gilt es darauf zu achten, eine sogenannte Krypto-Agilität – also die Fähigkeit, kryptografische Systeme und Sicherheitsmaßnahmen flexibel und anpassungsfähig zu gestalten – durch die Zentralisierung kryptographischer Funktionen zu schaffen. In diversen regulatorischen Direktiven (z.B. NIS2, CRA) und internationalen Standards (z.B. ISO27001) wird ein zukunftsorientierter Ansatz der Informationssicherheit gefordert. Auch wegen der im Juni 2025 gesetzten Ziele der Europäischen Kommission zur Erreichung von Post-Quantum Readiness bis 2035, bei kritischer Infrastruktur sogar schon bis 2030, sollte eine Migrationsstrategie möglichst bald erarbeitet und durchgeführt werden, um diese ambitionierten Ziele zu erreichen. Eines der ersten geforderten Ziele ist der Aufbau eines Kryptographie-Inventars.

Kryptographie-Inventar

Ein Kryptografie-Inventar schafft Transparenz und eine klare Übersicht aller eingesetzten kryptografischen Verfahren, Schlüssel, Zertifikate und Algorithmen. Dadurch wird sichtbar, welche Sicherheitsmaßnahmen aktuell in einer Organisation verwendet werden. Durch die Dokumentation können veraltete oder unsichere Algorithmen (z.B. alte Verschlüsselungsstandards) identifiziert und ersetzt werden. Dadurch hilft es auch, Schwachstellen frühzeitig zu erkennen und gezielt zu beheben.

Viele regulatorische Vorgaben (z.B. DSGVO, ISO 27001, NIS2) verlangen Nachweise über den Einsatz geeigneter Verschlüsselungstechnologien. Auch durch die im Juni 2025 gesetzten Ziele der Europäischen Kommission zur Einrichtung eines Kryptographie-Inventars bis spätestens Ende 2026 sollte eine Umsetzungsstrategie zeitnah erfolgen.

Ein Inventar erleichtert die Einhaltung dieser Vorgaben durch dokumentierte Nachweise, wie eine Übersicht der genutzten Kryptographie inklusive Schlüsselinformation.

Durch die Kenntnis aller kryptografischen Komponenten kann das Risiko von Angriffen besser eingeschätzt werden. Ein Kryptografie-Inventar unterstützt daher auch bei der Planung von Sicherheitsmaßnahmen und Investitionen. Bei Umstellungen auf neue Standards oder Technologien erleichtert ein Inventar die Planung und Umsetzung. Es sorgt für Kontinuität und minimiert Ausfallzeiten. Des Weiteren kann im Falle eines Sicherheitsvorfalls schnell nachvollzogen werden, welche Daten und welche Verschlüsselungstechnologien betroffen sind.

Letztendlich fördert ein Kryptografie-Inventar den Aufbau einer Sicherheitskultur, denn das Bewusstsein für den Einsatz kryptografischer Maßnahmen wird erhöht und Verantwortlichkeiten werden klar definiert.

Quantum Key Distribution

Bei der sogenannten Quantum Key Distribution (QKD) handelt es sich um eine Methode, bei der Quantenmechanik genutzt wird, um eine sichere Kommunikation zu gewährleisten. Im Wesentlichen ermöglicht QKD den Austausch von Verschlüsselungsschlüsseln zwischen zwei Parteien auf eine Weise, die es sehr schwer macht, den Schlüssel abzufangen oder zu manipulieren. Das Besondere daran ist, dass durch die Prinzipien der Quantenphysik jeder Abhörversuch sofort bemerkt werden würde, weil die Messung eines Quantenzustands den Zustand des Schlüssels verändert. So kann man sicherstellen, dass der Schlüssel wirklich geheim bleibt.

Mit dem Einsatz von effektiven Schutzmechanismen im Bereich der PQC und der QKD-Technologie kann der Datenaustausch zwischen verschiedenen Standorten oder zwischen Unternehmen, Kunden und Partnern für die Zukunft abgesichert werden. Zielgruppen für den Einsatz einer QKD-Technologie können On-Prem- und/oder Cloud-Native-Rechenzentren und Public-Cloud-Szenarien sein, jeweils mit dem Fokus auf extern zugängliche Systeme.

Ziele einer Migration auf Basis einer QKD-Implementierung in Unternehmen

Das Ziel einer QKD-Implementierung im Zuge einer Post-Quantum Migration in Unternehmen ist das Erreichen von Quantensicherheit bei der Schlüsselvereinbarung von Systemen, die dem Internet und damit einem SDNL-Bedrohungsszenario ausgesetzt sind. Ein weiteres wichtiges Ziel ist die Bewusstseinsbildung für den Bedarf einer post-quantensicheren Migration von Informationssystemen, Daten und Kommunikationsprotokollen bei Geschäftsführern, Managern, Mitarbeitern und Partnern. Ein letzter Punkt ist die Planung weiterer Phasen zur Erreichung von Quanten-Resilienz für andere kryptografische Verfahren, wie z.B. für digitale Signaturen und ggf. für die Umstellung der Softwarearchitektur.

Welche Maßnahmen sind bei einer Post-Quantum Migration umzusetzen?

Im Wesentlichen gilt es, bei einer Post-Quantum Migration fünf grundlegende Maßnahmen umzusetzen: Zunächst sollte die Erstellung eines Kryptographie-Inventars erfolgen, das alle kryptographischen Assets umfasst. Wie bereits erläutert, bietet ein Kryptographie-Inventar Organisationen

eine strukturierte Übersicht ihrer kryptografischen Maßnahmen, verbessert die Sicherheit, erleichtert Compliance, unterstützt bei der Priorisierung während der PQ-Migration und darüber hinaus und trägt insgesamt zu einem systematischen Schutz sensibler Daten bei.

In einem zweiten Schritt folgt dann die Umstellung der betrachteten Systeme auf standardisierte PQC-Algorithmen in Kombination mit klassischen Verfahren, bevor die Definition und Implementierung einer "Out-of-Band-Kryptoschicht" erfolgt – einer Sicherheits- oder Verschlüsselungsschicht, die außerhalb des regulären Datenflusses liegt und dazu dient, die Sicherheit der Kommunikation zu erhöhen. Sie findet z.B. Anwendung bei der Authentifizierung, in dem ein zweiter Kanal genutzt wird, um Identitäten oder Transaktionen zu bestätigen (z.B. Hardware-Token) oder bei einem QKD-Schlüsselaustausch, bei dem Schlüssel über einen separaten Kanal übertragen werden, um Abhörversuche im Hauptkanal zu verhindern, oder bei der Verifikation, bei der Bestätigungen oder Zertifikate außerhalb des normalen Kommunikationspfades überprüft werden.

In einem nächsten Schritt erfolgt dann die Planung eines Kryptolayers für unternehmenseigene Anwendungen. Ein Kryptolayer ist eine abstrakte Schicht in der Software, die Verschlüsselung, Entschlüsselung, Schlüsselmanagement und andere kryptografische Funktionen kapselt. Er sorgt dafür, dass diese Sicherheitsmaßnahmen zentralisiert und standardisiert innerhalb der Anwendung umgesetzt werden. Der Hauptzweck eines Kryptolayers ist es, die Sicherheit der Daten zu gewährleisten, ohne dass die eigentliche Anwendungslogik direkt mit den kryptografischen Details interagieren muss. Das erhöht die Sicherheit, Wartbarkeit und Flexibilität der Anwendung.

Die vier Phasen einer Post-Quantum Migration

Eine Post-Quantum Migration lässt sich in die vier Phasen Diagnose, Planung, Ausführung, und Wartung unterteilen. Die Diagnose ist die erste Phase, in der ein Migrationsteam alle relevanten Informationen über die vorhandene Infrastruktur sammelt und alle kryptographischen Verfahren, die für Quantenalgorithmen anfällig sind (einschließlich der Zuweisungen zu Geschäftsprozessen, zu Geschäftsdiensten und zu Infrastrukturdiensten) identifiziert. Für eine erfolgreiche Post-Quantum-Migration ist eine enge Abstimmung zwischen einem strategischen Top-Down-Ansatz, der die Gesamtstrategie und Governance festlegt, und einem praktischen Bottom-Up-Ansatz, der die technische Implementierung und Integration sicherstellt, unabdingbar.

In der Planungsphase wird der Migrationsprozess unter Berücksichtigung der zuvor gesammelten Informationen konzipiert und priorisiert, geeignete Tools und Ansätze zur Erstellung eines Kryptografie-Inventars bewertet und ausgewählt, sowie ein „Fahrplan“ zur Migration erstellt. Die Ausführung besteht in der eigentlichen Migration aller kryptographischen Verfahren, die für Quantenalgorithmen anfällig sind und der kontinuierlichen Pflege des Krypto-Inventars.

Die letzte Phase des Migrationsprozesses, die Wartung der gesamten betroffenen Infrastruktur, ist eine laufende Phase, die bereits mit der Ausführung beginnt. Sie ist in der Tatsache begründet, dass sich die betrachtete Infrastruktur im Laufe der Zeit verändert, sowohl während der Ausführungsphase als auch danach. Daher muss eine kontinuierliche Anpassung erfolgen und die Infrastruktur entsprechend „eingestellt“ werden.

Zusammenfassung

Die Kryptographie mit öffentlichen Schlüsseln ist für die Sicherung einer breiten Palette von Diensten, die sich direkt auf unser tägliches Leben auswirken, von entscheidender Bedeutung. Dazu gehören beispielsweise die Wahrung von Geschäftsgeheimnissen, von Gesundheits- und Persönlichkeitsdaten, die Überweisung von Geld von einem Bankkonto, die Unterzeichnung eines digitalen Vertrags oder generell die sichere Übertragung und Speicherung von Daten. Würden die derzeit eingesetzten Public-Key-Verfahren gebrochen, hätte das verheerende Folgen für unsere öffentliche digitale Infrastruktur. Diese Bedrohung für die Kryptografie geht von der Entwicklung eines großen fehlertoleranten Quantencomputers aus, der aufgrund des Shor-Algorithmus herkömmliche Verschlüsselungsverfahren mit öffentlichen Schlüsseln brechen kann, die beispielsweise auf RSA oder elliptischer Kurvenverschlüsselung (ECC) basieren. Solche kryptographisch relevanten Quantencomputer (CRQC) sind derzeit noch nicht verfügbar, ihre Entwicklung schreitet jedoch rasch voran.

Daher sollte die Vorbereitung auf die Quantenbedrohung als integraler Aspekt des Risikomanagements im Bereich der Cybersicherheit angesehen werden. In einem Versuch, das Risiko zu quantifizieren, wurde in der Ausgabe 2024 des Quantum Threat Timeline Reports des Kanadischen Global Risk Institute eine Umfrage unter 32 international führenden Experten aus Wissenschaft und Industrie durchgeführt. Die Experten wählten Wahrscheinlichkeitsbereiche für die Realisierung eines kryptorelevanten Quantencomputers innerhalb verschiedener Zeitrahmen von 5 bis 30 Jahren. Eine "optimistische" Interpretation der Antworten führte im Durchschnitt zu einer Schätzung von ~34 %, dass ein CRQC innerhalb eines Jahrzehnts entwickelt wird (gegenüber 31 % im Jahr 2023), und ~14 % innerhalb von 5 Jahren (gegenüber 11 % im Jahr 2023). Selbst eine "pessimistische" Interpretation ergab eine durchschnittliche Wahrscheinlichkeitsschätzung von ~19% für eine disruptive Quantenbedrohung in den nächsten 10 Jahren.

Mehrere gut untersuchte Alternativen der Post-Quantum-Kryptografie (PQC) zu derzeit eingesetzten Kryptografieverfahren sind entweder bereits standardisiert oder stehen kurz vor der Standardisierung und sind für den Einsatz in der Produktion bereit. Da sie jedoch noch relativ neu sind und die Erfahrung mit ihrer Implementierung und Kryptoanalyse noch nicht ausgereift ist, empfehlen wir derzeit für die meisten Anwendungsfälle den Einsatz von PQC in hybriden Lösungen, d.h. die Kombination eines eingesetzten kryptografischen Schemas mit PQC in einer Weise, dass die Kombination auch dann sicher bleibt, wenn eine ihrer Komponenten gebrochen wird.

In einer gemeinsamen Erklärung vom November 2024 unter dem Vorsitz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), dem Niederländischen Innenministerium und der Französischen Nationalen Agentur für die Sicherheit von Informationssystemen wird gemeinsam mit weiteren Partnern aus insgesamt 18 EU-Mitgliedstaaten einen sofortigen Übergang zur Post-Quantum-Kryptographie einzuleiten. Zusätzlich wird in diversen regulatorischen Direktiven (z.B. NIS2, CRA) und internationalen Standards (z.B. ISO27001) ein zukunftsorientierter Ansatz der Informationssicherheit gefordert.

Des Weiteren stellte die Europäische Kommission am 23. Juni 2025 einen koordinierten Fahrplan für die Umstellung der digitalen Infrastruktur Europas auf die Post-Quanten-Kryptografie (PQC) vor. Dieser enthält einen Zeitplan für die Umstellung auf quantenresistente Verschlüsselung. Dabei wurden folgende Meilensteine für einen PQC-Übergangszeitplan von der EU definiert:

- Bis Ende 2026: Alle EU-Mitgliedstaaten sind aufgefordert mit der Umstellung auf PQC zu beginnen, indem sie nationale Strategien und "erste Schritte" für die Migration einleiten. Dies bedeutet, dass spätestens 2026 mit Bewertungen, Sensibilisierungskampagnen und kryptografischen Bestandsaufnahmen begonnen werden muss.
- Bis Ende 2030: Systeme mit hohem Risiko - insbesondere kritische Infrastrukturen und andere lebenswichtige Sektoren - müssen so schnell wie möglich, spätestens jedoch bis 2030, mit Post-Quantum-Kryptografie gesichert werden.
- Bis 2035: Der Übergang zu PQC sollte für so viele Systeme wie praktisch möglich in ganz Europa abgeschlossen sein. Dieses ehrgeizige Ziel für 2035 räumt ein, dass einige ältere oder weniger risikobehaftete Systeme länger brauchen könnten, aber sie sollten bis dahin so weit wie möglich quantensicher sein.

Wenn ein Unternehmen digitalisierte Geschäftsprozesse nutzt, dann werden derzeit mit sehr hoher Wahrscheinlichkeit für die Bedrohung durch Quantencomputer anfällige, asymmetrische kryptografische Verfahren für die Cybersicherheit eingesetzt. Daher können es sich Unternehmen nicht leisten, auf das Aufkommen von Quantencomputern zu warten. Unternehmen sind daher gut beraten, folgende Maßnahmen zu ergreifen:

- Sie sollten sicherstellen, dass sie über ein aktuelles, gründliches Unternehmensinventar verfügen, das Einzelheiten über genutzte, wie eingebettete, Kryptografie enthält, die in einer Vielzahl von Produkten vorhanden sein kann.
- Sie sollten ihre Systeme und IT-Assets auf Bedrohungen überwachen und sicherstellen, dass regelmäßige Risikobewertungen durchgeführt werden.
- Sie sollten eine Quantum-Risikobewertung als Teil des regulären Risikobewertungsprozesses oder im Anschluss an diesen durchführen.
- Sie sollten sich über die Einstellung ihrer Telekommunikations- und Sicherheitsanbieter in Bezug auf Quantencomputing informieren, welche ihrer Produkte davon betroffen sind und wie sie sich auf die Bewältigung Risikos durch kryptographisch relevante Quantencomputer vorbereiten.
- Sie sollten die Quantenbereitschaft als Teil ihrer aktuellen Beschaffungsprozesse für Netzwerk- und Sicherheitssysteme bewerten und ihre derzeitigen Anbieter bitten, den Stand ihrer Quantenplanung zu erörtern.
- Es empfiehlt sich mit einem sachkundigen Partner zusammenzuarbeiten, um die Entwicklungen im Bereich Quantencomputer und Quantensicherheitslösungen zu verfolgen und einen Fahrplan für die Quantenbereitschaft des Unternehmens zu erstellen.

Die wichtigste Botschaft lautet: Unternehmen müssen jetzt handeln! Die Organisationen, die am meisten gefährdet sind, sind diejenigen, die auf die Ankunft von kryptographisch relevanten Quantencomputern warten oder Maßnahmen vermeiden, bis perfekte kryptografische Lösungen entwickelt sind. Dies wird mit ziemlicher Sicherheit dazu führen, dass eine Organisation in absehbarer Zeit mit ihrer plötzlichen Anfälligkeit für Quantenangriffe zu kämpfen hat.

Verweise

18 EU member states. (2024, 11 30). *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*. Veröffentlicht auf www.bsi.bund.de: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

Dr. Michele Mosca, D. M. (2024, 12 06). *Quantum Threat Timeline Report 2024*. Veröffentlicht auf globalriskinstitute.org: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

Dr. Michele Mosca, J. M. (2022, 11 09). *A Methodology for Quantum Risk Assessment - Global Risk Institute*. Veröffentlicht auf globalriskinstitute.org: https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/

FS-ISAC's Post-Quantum Cryptography Working Group. (2023, 03). *Preparing for a Post-Quantum World by Managing Cryptographic Risk*. Veröffentlicht auf www.fsisac.com: https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForAPostQuantumWorldByManagingCryptographicRisk.pdf

NIS Cooperation Group. (2025, 06 23). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. Veröffentlicht auf digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR). (2024, 07 10). *Canadian National Quantum-Readiness - BEST PRACTICES AND GUIDELINES*. Veröffentlicht auf https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

SAMA PARTNERS – Ihr Partner für Informationssicherheit, künstliche Intelligenz und Compliance

SAMA PARTNERS ist ein unabhängiges IT-Beratungs- und Engineering-Unternehmen mit Hauptsitz in Mannheim mit den Schwerpunkten Informationssicherheit, KI und Compliance, das langjährige Branchenkompetenz im Bereich der IT-Sicherheit mit integrierten Security-Operations-Lösungen vereint. Seit 2010 unterstützen wir Manager, Sicherheits- und IT-Verantwortliche dabei, die Cyber-Risiken in ihren Unternehmen zu bewerten und deren Behandlung zu einer organisatorischen Priorität zu machen.

SAMA PARTNERS hat gemeinsam mit dem Kanadisch-Deutschen Unternehmen evolutionQ als strategischem Partner bereits erste Assessments und Inventarisierungen im Krypto-Umfeld erfolgreich durchgeführt. Unser Ansatz: Wir unterstützen Unternehmen dabei, Risiken und Potenziale im Kontext von Krypto-Systemen, Assets und Post-Quantum-Readiness frühzeitig zu erkennen und diese gezielt zu adressieren.

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY